UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION	))	MDL No. 1:19md2915 (AJT/JFA)

AMAZON DEFENDANTS' OBJECTIONS AND RESPONSES TO PLAINTIFFS' FIRST INTERROGATORIES

Pursuant to Rules 26 and 33 of the Federal Rules of Civil Procedure and Local Civil Rule 26(c), Defendants Amazon.com, Inc. and Amazon Web Services, Inc. (collectively "Amazon" or "Amazon Defendants") hereby respond to Plaintiffs' First Set of Interrogatories (Nos. 1 – 20) as follows:

PRELIMINARY STATEMENT

Amazon Defendants' investigation in this action is ongoing, and Amazon Defendants reserve the right to rely on and introduce information in addition to any information provided in response to the Interrogatories at the trial of this matter or in other related proceedings. A representative complaint has not yet been filed, and Amazon Defendants have yet to complete their investigation, or receive the benefit of expert opinion and analysis, and/or discovery from Plaintiffs and other parties. Amazon Defendants anticipate that information they discover later in the litigation may be responsive to one or more of the Interrogatories, and Amazon Defendants reserve their right to supplement their responses at appropriate points throughout this litigation without prejudice and/or to otherwise make available to Plaintiffs such information. Amazon Defendants also reserve the right to change, modify, or enlarge the following objections and/or responses based on amendments to pleadings, additional information, further analysis, and/or in light of other events in the litigation. Unless specifically stated otherwise in the individual responses to the Interrogatories, Amazon Defendants' statement on supplementation applies to all of them.

OBJECTIONS TO DEFINITIONS

1. Amazon Defendants object to the definitions of "PII" as vague, ambiguous, uncertain, and calling for information that is not within Amazon Defendants' possession, custody, or control. Amazon Defendants further object to the definition of "PII" as overbroad, unduly burdensome, and disproportionate to the needs of the case to the extent that it is more expansive than, or inconsistent with, the meaning of those terms as used in Amazon's ordinary course of business or as defined by relevant statutes or regulations applicable to Amazon's business.

2. Amazon Defendants object to the definitions of "Amazon," "Amazon Web Services," "AWS, "You," and "Your" as overbroad and unduly burdensome to the extent that it purports to extend to persons or entities outside of Amazon Defendants' control, and, specifically, as it seeks discovery from Amazon Defendants' "former directors, officers, employees, agents, representatives or any persons acting or purporting to act on Amazon's behalf."

3. Amazon Defendants object to the time frame of January 1, 2015 through the present as overbroad and unduly burdensome to the extent that they request information outside of a time period relevant to the action. Amazon Defendants object to the definition of the "Relevant Period" as overbroad, unduly burdensome, and disproportionate to the needs of the case to the extent that it includes information or documents created or generated after the filing of the first complaints in this litigation on July 30, 2019. Amazon Defendants further object to the definition of the "Relevant Period" to the extent it includes "responsive Documents created or generated outside the Relevant Period, but which contain information concerning the Relevant Period," because (i) the phrase "information concerning the Relevant Period" is vague and ambiguous and, moreover, (ii) this portion of the definition effectively expands the scope of the "Relevant Period" to include an unlimited period of time.

SPECIFIC OBJECTIONS AND RESPONSES TO INTERROGATORIES

INTERROGATORY NO. 1:

Identify the individuals responsible for Your data security protocols and procedures, including Your data security officers, for Your AWS cloud product, including the individuals responsible for Capital One's AWS cloud.

OBJECTIONS TO INTERROGATORY NO. 1:

Amazon Defendants object to the Interrogatory as overly broad, unduly burdensome and not proportional to the needs of the case in that the Interrogatory broadly seeks information that is not appropriately limited to (i) the 2019 cybersecurity incident (and impacted Capital One systems / information); (ii) AWS products and services used by Capital One; and/or (iii) the claims and defenses in the litigation. Amazon Defendants object to this Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly burdensome to the extent that it requests information outside of a time period relevant to the action. Amazon Defendants object to this Interrogatory as vague, overbroad and unduly burdensome to the extent it seeks information regarding each and every individual "responsible for . . . data security protocols and procedures." Amazon Defendants object to "AWS cloud product" as vague, ambiguous and overly broad; Amazon offers more than 175 services through AWS and responding for each service would be unduly burdensome and not proportionate to the needs of the case. Amazon Defendants object to "Your data security officers" as vague and ambiguous.

RESPONSES TO INTERROGATORY NO. 1:

Subject to the foregoing objections, Amazon responds as follows:

Amazon and its AWS customers, including Capital One, employ a Shared Responsibility Model for security of data stored in AWS. Under this model, AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Security is at the core of AWS's business, and numerous AWS employees across the globe have responsibility for security of the cloud infrastructure that AWS manages. AWS's Chief Information Security Officer is Stephen Schmidt.

The customer, in this case Capital One, assumes responsibility and management for the security of the guest operating system (including updates and security patches), other associated application software as well as the configuration of its web application firewall, which, in this case, was a third-party application firewall not provided by Amazon. Amazon offers AWS customers a suite of security and data protection services that they can choose to use in their environments. These services are described in detail at https://aws.amazon.com/products/security/.

The data security event described in Capital One's July 29, 2019 press release (the "Data Breach") concerned access to Capital One data through a Capital One web application and not through a breach of the underlying AWS cloud-based infrastructure. This type of vulnerability is not specific to the cloud.

INTERROGATORY NO. 2:

Identify the individuals responsible for Your use, including the set-up, implementation, logging, and monitoring, of Capital One's AWS cloud instances and services.

OBJECTIONS TO INTERROGATORY NO. 2:

Amazon Defendants object to this Interrogatory as unintelligible, as Amazon does not "use" Capital One's AWS cloud instances and services. Amazon Defendants object to the Interrogatory as overly broad, unduly burdensome and not proportional to the needs of the case in

that the Interrogatory broadly seeks information that is not appropriately limited to (i) the 2019 cybersecurity incident (and impacted Capital One systems / information); (ii) AWS products and services used by Capital One; and/or (iii) the claims and defenses in the litigation. Amazon Defendants object to this Interrogatory to the extent that it seeks information that is more readily accessible to Capital One, which has control of its AWS environment. Amazon Defendants object to "individuals responsible for Your use" and "Capital One's AWS cloud instances and services" as vague, ambiguous, overbroad and unduly burdensome. The terms "logging" and "monitoring" are similarly vague, ambiguous, and capable of various interpretations. The Interrogatory is also overbroad, unduly burdensome, and disproportionate to the needs of the case because it asks Amazon Defendants to provide an exhaustive list identifying each and every individual who performed work relating to Capital One's use of AWS cloud services over a more than five-year period.

RESPONSES TO INTERROGATORY NO. 2:

Subject to the foregoing objections, Amazon responds as follows:

Amazon and its AWS customers, including Capital One, employ a Shared Responsibility Model for security of data stored in AWS. Under this model, AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer, in this case Capital One, assumes responsibility and management for the security of the guest operating system (including updates and security patches), other associated application software as well as the configuration of its web application firewall, which, in this case, was a third-party application firewall not provided by Amazon. Pursuant to Federal Rule of Civil Procedure 33(d), Amazon will produce documents sufficient to show the principle members of the AWS account team for Capital One.

INTERROGATORY NO. 3:

Describe in detail Your AWS cloud environment, providing details of the components of the network and any connected systems or servers used to process and/or store any PII. Such description and/or diagram shall include the location (within the network) of computer systems; servers; firewalls; routers; internet; private lines and other connections; all buckets, instances, connections to any internal and external network; virtual private network; remote access equipment (such as wireless access points); WAFs, APIs, websites; and security mechanisms and devices (such as intrusion detection systems).

OBJECTIONS TO INTERROGATORY NO. 3:

Amazon Defendants object to the Interrogatory as overly broad, unduly burdensome and not proportional to the needs of the case in that the Interrogatory broadly seeks information that is not appropriately limited to (i) the 2019 cybersecurity incident (and impacted Capital One systems / information); (ii) AWS products and services used by Capital One; and/or (iii) the claims and defenses in the litigation. Amazon has more than one million AWS customers, and, as written, this Interrogatory calls for a description "in detail" of the AWS cloud environment as to all of these customers, in addition to Capital One. Amazon Defendants object to "AWS cloud environment" as vague, ambiguous and overly broad; Amazon offers more than 175 services through AWS and responding for each service would be unduly burdensome and not proportionate to the needs of the case. Amazon Defendants further object to this Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly burdensome to the extent that it requests information outside of a time period relevant to the action. Amazon Defendants object to the Interrogatory because it incorporates the defined term "PII" for the reasons set forth in the Objections to Definitions above.

Amazon Defendants further object to the Interrogatory because a number of the terms and phrases it contains—including "computer network," "internet," "private lines and other connections," and "security mechanisms and devices"—are vague, ambiguous, and capable of various interpretations.

RESPONSES TO INTERROGATORY NO. 3:

Subject to the foregoing objections, Amazon responds as follows:

Pursuant to Federal Rule of Civil Procedure 33(d), in response to this interrogatory, Amazon refers to https://aws.amazon.com/, which provides detailed documentation and descriptions of the AWS services.

INTERROGATORY NO. 4:

Describe in detail Capital One's AWS cloud, including its configuration and changes (if any) made to the default configuration since 2016.

OBJECTIONS TO INTERROGATORY NO. 4:

Amazon Defendants object to the Interrogatory as overly broad, unduly burdensome and not proportional to the needs of the case in that the Interrogatory broadly seeks information that is not appropriately limited to (i) the 2019 cybersecurity incident (and impacted systems / information) and/or (ii) the claims and defenses in the litigation. Amazon Defendants object to this Interrogatory to the extent that it seeks information that is more readily accessible to Capital One, which has control of its AWS environment. Amazon Defendants object to this Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly burdensome to the extent that it requests information outside of a time period relevant to the action. Amazon Defendants object to this Interrogatory as compound and unintelligible. Amazon Defendants object to "configuration

and changes" vague, ambiguous, and overly broad to the extent that it seeks "configurations and changes" unrelated to the Breach. Amazon Defendants object to "default configuration" as vague and ambiguous.

RESPONSES TO INTERROGATORY NO.4:

Subject to foregoing objections, Amazon responds as follows:

Amazon and its AWS customers, including Capital One, employ a Shared Responsibility Model for security of data stored in AWS. Under this model, AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer, in this case Capital One, assumes responsibility and management for the guest operating system (including updates and security patches), other associated application software as well as the configuration of the guest operating system and its applications. The configuration of Capital One's AWS instances is the responsibility of Capital One.

INTERROGATORY NO. 5:

Identify all third-party entities that provide computer network and computer system security-related services to You with respect to Your AWS cloud product, as well as what services each such third-party entity provides to You and the dates they provided such services.

OBJECTIONS TO INTERROGATORY NO. 5:

Amazon Defendants object to the Interrogatory as overly broad, not relevant to any claim or defense in this action, unduly burdensome and not proportional to the needs of the case in that the Interrogatory broadly seeks information that is not appropriately limited to (i) the 2019 cybersecurity incident (and impacted Capital One systems / information); (ii) AWS products and services used by Capital One; and/or (iii) the claims and defenses in the litigation. Amazon has

more than one million AWS customers, and, as written, this Interrogatory calls for identification of all third parties that provide computer network and computer system security-related services regarding AWS. Amazon Defendants object to "AWS cloud product" as vague, ambiguous and overly broad; Amazon offers more than 175 services through AWS and responding for each service would be unduly burdensome and not proportionate to the needs of the case. Amazon Defendants object to the Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly burdensome to the extent that it requests information outside of a time period relevant to the action. Amazon Defendants object to the Interrogatory because the phrase "computer network and computer system security-related services" is vague, ambiguous, and capable of various interpretations.

RESPONSES TO INTERROGATORY NO. 5:

Amazon stands on its objections to this interrogatory.

INTERROGATORY NO. 6:

Describe in detail Your use of a penetration testing team, cyber security threat intelligence program, or ethical hacks in Your AWS cloud environment, including tests of Capital One's AWS cloud environment, and web applications by vendors or internal teams, including the results of any such testing.

OBJECTIONS TO INTERROGATORY NO. 6:

Amazon Defendants object to the Interrogatory as overly broad, not relevant to any claim or defense in this action, unduly burdensome and not proportional to the needs of the case in that the Interrogatory broadly seeks information that is not appropriately limited to (i) the 2019 cybersecurity incident (and impacted Capital One systems / information); (ii) AWS products and

services used by Capital One; and/or (iii) the claims and defenses in the litigation. Amazon Defendants object to "Your AWS cloud environment" as vague, ambiguous and overly broad; Amazon offers more than 175 services through AWS and responding for each service would be unduly burdensome and not proportionate to the needs of the case. Amazon Defendants object to this Interrogatory to the extent that it seeks information that is more readily accessible to Capital One, which has control of its AWS environment. Amazon Defendants further object to this Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly burdensome to the extent that it requests information outside of a time period relevant to the action. Amazon Defendants object to this Interrogatory as compound and consisting of at least four distinct subparts. Amazon Defendants object to this Interrogatory to the extent it seeks disclosure of information that is protected from disclosure by the attorney-client privilege, attorney work product doctrine, joint defense privilege, common interest exception, or any other applicable privilege, immunity, doctrine or protection. Amazon Defendants object to the Interrogatory because the terms "cyber security threat intelligence program" and "ethical hacks" are vague, ambiguous, and capable of various interpretations.

RESPONSES TO INTERROGATORY NO. 6:

Subject to the foregoing objections, Amazon responds as follows:

Amazon and its AWS customers, including Capital One, employ a Shared Responsibility Model for security of data stored in AWS. Under this model, AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer, in this case Capital One, assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS

provided security group firewall. To the extent any penetration testing or ethical hacking was performed on Capital One's AWS instances, such testing would be within the knowledge of Capital One.

INTERROGATORY NO. 7:

Describe in detail each instance in which You received notice of any kind related to the Breach or the possibility that a third-party had obtained unauthorized access to Capital One's AWS cloud environment and the remedial action (if any) You took in response. Your answer shall include how, when, and through whom You received notice, as well as describe the software or the manner in which You received such notification.

OBJECTIONS TO INTERROGATORY NO. 7:

Amazon Defendants object to this Interrogatory to the extent it seeks disclosure of information that is prohibited from disclosure pursuant to a court-issued non-disclosure order. Amazon Defendants object to this Interrogatory to the extent it seeks disclosure of information that is protected from disclosure by the attorney-client privilege, attorney work product doctrine, joint defense privilege, common interest exception, or any other applicable privilege, immunity, doctrine or protection.

RESPONSES TO INTERROGATORY NO.7:

Subject to the foregoing objections, Amazon responds as follows:

Capital One notified AWS's Chief Information Security Officer, Stephen Schmidt, of the Data Breach on July 20, 2019.

INTERROGATORY NO. 8:

Describe in detail each instance in which You received notice of any kind related to Your AWS cloud product and the remedial action (if any) You took in response. Your answer shall include how, when, and through whom You received notice, as well as describe the software or the manner in which You received such notification.

OBJECTIONS TO INTERROGATORY NO. 8:

Amazon Defendants object to the Interrogatory as overly broad, unduly burdensome and not proportional to the needs of the case in that the Interrogatory broadly seeks information that is not appropriately limited to (i) the 2019 cybersecurity incident (and impacted Capital One systems / information); (ii) AWS products and services used by Capital One; and/or (iii) the claims and defenses in the litigation. Amazon objects to the Interrogatory to the extent it seeks information regarding "notice of any kind" of unrelated incidents or potential incidents involving systems and/or vulnerabilities unrelated to the Breach. Amazon has more than one million AWS customers, and, as written, this Interrogatory calls for Amazon to describe in detail any notice of any kind it has received, regardless of its relation to the Capital One data breach at issue in this case. Amazon Defendants object to "AWS cloud product" as vague, ambiguous and overly broad; Amazon offers more than 175 services through AWS and responding for each service would be unduly burdensome and not proportionate to the needs of the case. Amazon Defendants further object to this Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly burdensome to the extent that it requests information outside of a time period relevant to the action. Amazon Defendants object to this Interrogatory as compound and consisting of at least two distinct subparts. Amazon Defendants object to this Interrogatory to the extent it seeks disclosure of information that is protected from disclosure by the attorney-client privilege, attorney work product doctrine, joint defense privilege, common interest exception, or any other applicable privilege, immunity, doctrine or protection.

RESPONSES TO INTERROGATORY NO. 8:

Subject to the foregoing objections, Amazon responds as follows:

Amazon responds that it will meet and confer concerning the topic of the "notice of any kind."

INTERROGATORY NO. 9:

Describe in detail Paige Thompson's creation of temporary and permanent credentials and use of those credentials to access Capital One's AWS system, including detailing the dates of access, information accessed, and information downloaded.

OBJECTIONS TO INTERROGATORY NO. 9:

Amazon Defendants object to this Interrogatory to the extent it seeks information that is equally available to Plaintiffs from other sources that are more convenient, less burdensome and/or less expensive; are already in their possession; or are publicly available. Amazon Defendants object to this Interrogatory to the extent that it seeks information that is more readily accessible to Capital One, which has control of its AWS environment. Amazon Defendants object to this Interrogatory because the phrase "temporary and permanent credentials" is vague, ambiguous, and capable of various interpretations. Amazon Defendants object to this Interrogatory to the extent it seeks disclosure of information that is protected from disclosure by the attorney-client privilege, attorney work product doctrine, joint defense privilege, common interest exception, or any other applicable privilege, immunity, doctrine or protection.

RESPONSES TO INTERROGATORY NO.9:

Subject to the foregoing objections, Amazon responds as follows:

The Data Breach concerned access to Capital One data through a Capital One web application and not through a breach of the underlying AWS cloud-based infrastructure. This type of vulnerability is not specific to the cloud. Details on how and when those credentials were used within Capital One's AWS environment would, if known, be known to Capital One.

INTERROGATORY NO. 10:

Identify each location or component of Capital One's AWS cloud on which PII was or may have been accessed during the Breach. For each such location or component, describe: the type(s) and amount(s) of accessed data; the file name and size containing such data; the manner by which unauthorized access was made, and the time period during which such unauthorized access occurred.

OBJECTIONS TO INTERROGATORY NO. 10:

Amazon Defendants object to this Interrogatory to the extent that it seeks information that is more readily accessible to Capital One, which has control of its AWS environment. Amazon Defendants object to the Interrogatory as overly broad, unduly burdensome and not proportional to the needs of the case in that the Interrogatory broadly seeks information that is not appropriately limited to the 2019 cybersecurity incident (and impacted Capital One systems / information). Amazon Defendants object to this Interrogatory as overly broad and without reasonable limitation in its time period or scope. Amazon Defendants object to the Interrogatory because it incorporates the defined term "PII" for the reasons set forth in the Objections to Definitions above. Amazon Defendants object to this Interrogatory to the extent it seeks information that is equally available to Plaintiffs from other sources that are more convenient, less burdensome and/or less expensive. Amazon Defendants object to this Interrogatory as compound and consisting of at least two distinct subparts. Amazon Defendants further object to the Interrogatory because the phrase "file name and size containing such data" is vague, ambiguous, and capable of various interpretations. Amazon Defendants object to this Interrogatory to the extent it seeks disclosure of information that is protected from disclosure by the attorney-client privilege, attorney work product doctrine, joint defense privilege, common interest exception, or any other applicable privilege, immunity, doctrine or protection.

RESPONSES TO INTERROGATORY NO. 10:

Subject to the foregoing objections, Amazon responds as follows:

The Data Breach concerned access to Capital One data through a Capital One web application and not through a breach of the underlying AWS cloud-based infrastructure. This type of vulnerability is not specific to the cloud. Details on data that was accessed within Capital One's AWS environment would, if known, be known to Capital One.

INTERROGATORY NO. 11:

Describe in detail any investigation You, or any third party on Your behalf, conducted into the Breach. Your answer shall include details of the persons (whether internal or external) involved in such investigation, their roles in the investigation, any agreements by which the investigation was conducted, the time during which the investigation was conducted, a description of any interviews, documentation, reports, and/or factual conclusions that You, or others acting on Your behalf, made as a result of such investigation, and a list of persons any report(s) were provided to as well as their employers and business titles.

OBJECTIONS TO INTERROGATORY NO. 2:

Amazon Defendants object to this Interrogatory as compound, calling for a narrative, and consisting of at least four distinct subparts. Amazon Defendants object to this Interrogatory because it seeks disclosure of information that is protected from disclosure by the attorney-client privilege, attorney work product doctrine, joint defense privilege, common interest exception, or any other applicable privilege, immunity, doctrine or protection. Amazon Defendants also object to the Interrogatory because the phrase "details of the persons" is vague and ambiguous, and fails to specify the information being sought.

RESPONSES TO INTERROGATORY NO. 11:

Subject to the foregoing objections, Amazon responds as follows:

The Data Breach concerned access to Capital One data through a Capital One web application and not through a breach of the underlying AWS cloud-based infrastructure. This type of vulnerability is not specific to the cloud. Because the Data Breach occurred within Capital One's AWS environment, Capital One led the investigation of the Data Breach.

INTERROGATORY NO. 12:

Describe in detail any remedial actions undertaken by You, or others acting on Your behalf, related to the Breach, including, without any limitation, any modification of Your policies, practices, procedures, hardware, software, and personnel for Your AWS cloud environments as used by Capital One and other customers, and the cost of those remediations.

OBJECTIONS TO INTERROGATORY NO. 2:

Amazon Defendants object to this Interrogatory to the extent it seeks disclosure of information that is protected from disclosure by the attorney-client privilege, attorney work product doctrine, joint defense privilege, common interest exception, or any other applicable privilege, immunity, doctrine or protection. Amazon Defendants further object to this Interrogatory because the term "cost" is vague, ambiguous, and capable of various interpretations in this context.

RESPONSES TO INTERROGATORY NO. 12:

Subject to the foregoing objections, Amazon responds as follows:

The Data Breach concerned access to Capital One data through a Capital One web application and not through a breach of the underlying AWS cloud-based infrastructure. This type of vulnerability is not specific to the cloud. In August 2019, AWS conducted a scan of public IP addresses of AWS enterprise accounts to identify potentially misconfigured firewalls and notified AWS customers of potential misconfigurations. Because Amazon does not know the business purposes behind each AWS customer's AWS environment, only the customer can determine whether a web application firewall was configured correctly.

INTERROGATORY NO. 13:

Describe the process by which You notified customers of Your AWS cloud product about the Breach, including the Date, manner, and content of each notification, the Person(s) responsible for drafting, reviewing, or otherwise creating each notification, and the information or data relied upon for each notification.

OBJECTIONS TO INTERROGATORY NO. 2:

Amazon Defendants object to "AWS cloud product" as vague, ambiguous and overly broad; Amazon offers more than 175 services through AWS. Amazon objects to this Interrogatory as compound and consisting of at least three distinct subparts. Amazon Defendants object to "otherwise creating" as vague and ambiguous. Amazon Defendants object to this Interrogatory to the extent it seeks disclosure of information that is protected from disclosure by the attorney-client privilege, attorney work product doctrine, joint defense privilege, common interest exception, or any other applicable privilege, immunity, doctrine or protection. Amazon Defendants object to the Interrogatory as overbroad, unduly burdensome, and disproportionate to the needs of the case to the extent that it requires Amazon Defendants to provide "the information or data relied upon for each notification" it made related to the Breach.

RESPONSES TO INTERROGATORY NO. 13:

Subject to the foregoing objections, Amazon responds as follows:

Amazon did not provide notices to AWS customers about the Breach. The Data Breach concerned access to Capital One data through a Capital One web application and not through a breach of the underlying cloud-based infrastructure that is under Amazon's possession. This type of vulnerability is not specific to the cloud.

INTERROGATORY NO. 14:

Identify all polices, both internal and customer-facing, relating to the security of PII for Your AWS cloud product, including the dates of implementation or changes to such policies.

OBJECTIONS TO INTERROGATORY NO. 2:

Amazon objects to the term "policies" as vague and ambiguous. Amazon Defendants object to the Interrogatory as overly broad, unduly burdensome and not proportional to the needs of the case in that the Interrogatory broadly seeks information that is not appropriately limited to (i) the 2019 cybersecurity incident (and impacted Capital One systems / information); (ii) AWS products and services used by Capital One; and/or (iii) the claims and defenses in the litigation. Amazon Defendants object to "AWS cloud product" as vague, ambiguous and overly broad; Amazon offers more than 175 services through AWS and responding for each service would be unduly burdensome and not proportionate to the needs of the case. Amazon Defendants object to this Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly burdensome to the extent that it requests information outside of a time period relevant to the action. Amazon Defendants object to the Interrogatory because it incorporates the defined term "PII" for the reasons set forth in the Objections to Definitions above.

RESPONSES TO INTERROGATORY NO. 14:

Subject to the foregoing objections, Amazon responds as follows:

Security is the top priority of AWS. Amazon's AWS infrastructure is built to satisfy the security requirements for the military, global banks, and other high-sensitivity organizations. AWS's cloud security tools include 230 security, compliance, and governance services and features. AWS supports 90 security standards and compliance certifications, and all 117 AWS

services that store customer data offer the ability to encrypt that data. These compliance standards and certifications are available at https://aws.amazon.com/compliance.

Amazon offers AWS customers a suite of security and data protection services that they can choose to use in their environments. These services are described in detail at https://aws.amazon.com/products/security/.

INTERROGATORY NO. 15:

Describe in detail whether and how You determined the earliest date that any PII was accessed during the Breach, as well as what You determined this Date to be and what information was accessed, including the size of the information accessed.

OBJECTIONS TO INTERROGATORY NO. 2:

Amazon objects to this interrogatory as compound and consisting of at least two distinct subparts. Amazon Defendants object to the Interrogatory because it incorporates the defined term "PII" for the reasons set forth in the Objections to Definitions above. Amazon Defendants object to "size of the information" as vague and ambiguous. Amazon Defendants object to this Interrogatory to the extent it seeks disclosure of information that is protected from disclosure by the attorney-client privilege, attorney work product doctrine, joint defense privilege, common interest exception, or any other applicable privilege, immunity, doctrine or protection. Amazon Defendants object to this Interrogatory to the extent that it seeks information that is more readily accessible to Capital One, which has control of its AWS environment.

RESPONSES TO INTERROGATORY NO. 15:

Subject to the foregoing objections, Amazon responds as follows:

The Data Breach concerned access to Capital One data through a Capital One web application and not through a breach of the underlying AWS cloud-based infrastructure. This type of vulnerability is not specific to the cloud. Because the Data Breach occurred within Capital

One's AWS environment, Capital One led the investigation of the Data Breach. Amazon does not access customer data within the customer's AWS instances and does not determine whether customer data is personally identifiable information.

INTERROGATORY NO. 16:

Describe in detail how much You budgeted and how much You actually spent on data security for Your AWS cloud product each year during the Relevant Period. If You spent more or less than was budgeted in any given year, please explain in detail the reasons for the reduced or increased spending on data security.

OBJECTIONS TO INTERROGATORY NO. 2:

Amazon Defendants object to this Interrogatory for its budgets and spending for AWS security are not relevant to any claim or defense in this action and overly broad. Amazon Defendants object to the Interrogatory as overly broad, unduly burdensome and not proportional to the needs of the case in that the Interrogatory broadly seeks information that is not appropriately limited to (i) the 2019 cybersecurity incident (and impacted Capital One systems / information); (ii) AWS products and services used by Capital One; and/or (iii) the claims and defenses in the litigation. Amazon Defendants object to "AWS cloud product" as vague, ambiguous and overly broad; Amazon offers more than 175 services through AWS and responding for each service, including services not used by Capital One, would be unduly burdensome and not proportionate to the needs of the case. Amazon Defendants object to this Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly burdensome to the extent that it requests information outside of a time period relevant to the action. Amazon Defendants also object to the Interrogatory because the phrase "how much You budgeted and how much You actually spent on data security"

is vague, ambiguous, and overly broad. Additionally, it would be unduly burdensome—if not impossible—to "explain in detail" every reason why budgeting on data security matters may have increased or decreased over the past five years.

RESPONSES TO INTERROGATORY NO. 16:

Amazon stands on its objections to this interrogatory.

INTERROGATORY NO. 17:

Describe any financial benefit or profit You received from helping build Capital One's cloud environment, including whether you received benefit from using the AWS Capital One cloud environment and data to promote Your security, privacy, and ability to host financial institutions' data using AWS cloud services; whether You benefitted from using Capital One to deploy beta or test services produced by You and which You used to advertise Your products; and whether You benefitted by using Capital One as a case study through which You used Capital One PII data in the data lake. To the extent that You did financially benefit, please identify any and all Persons involved.

OBJECTIONS TO INTERROGATORY NO. 3:

Amazon objects that its "financial benefit or profit" from having Capital One as an AWS customer is not relevant to any claim or defense in the action. Amazon Defendants object to this Interrogatory on the grounds that it seeks information that is irrelevant, immaterial or not proportional to the needs of the case. Amazon Defendants object to the Interrogatory as overly broad, unduly burdensome to the extent that it seeks to identify "any and all Persons involved" in the multiple scenarios the Interrogatory presents. Amazon Defendants object to this Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly burdensome to the extent that it

requests information outside of a time period relevant to the action. Amazon Defendants object to this Interrogatory as compound and consisting of at least two distinct subparts. Defendants object to the Interrogatory because it incorporates the defined term "PII" for the reasons set forth in the Objections to Definitions above.

RESPONSES TO INTERROGATORY NO. 17:

Amazon stands on its objections to this interrogatory.

INTERROGATORY NO. 18:

Describe in detail all actions You took to test, validate, and/or monitor Your AWS cloud product, including Capital One's AWS cloud, including the results of any such tests.

OBJECTIONS TO INTERROGATORY NO. 4:

Amazon Defendants object to the Interrogatory as overly broad, not relevant to any claim or defense in this action, unduly burdensome and not proportional to the needs of the case in that the Interrogatory broadly seeks information that is not appropriately limited to (i) the 2019 cybersecurity incident (and impacted Capital One systems / information); (ii) AWS products and services used by Capital One; and/or (iii) the claims and defenses in the litigation. Amazon Defendants object to "AWS cloud product" as vague, ambiguous and overly broad; Amazon offers more than 175 services through AWS and responding for each service, including services not used by Capital One, would be unduly burdensome and not proportionate to the needs of the case. Amazon Defendants object to this Interrogatory to the extent that it seeks information that is more readily accessible to Capital One, which has control of its AWS environment. Amazon Defendants object to this Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly

burdensome to the extent that it requests information outside of a time period relevant to the action. Amazon Defendants object to this Interrogatory as compound, complex, and unintelligible.

RESPONSES TO INTERROGATORY NO. 18:

Subject to the foregoing objections, Amazon responds as follows:

The Data Breach concerned access to Capital One data through a Capital One web application and not through a breach of the underlying AWS cloud-based infrastructure. This type of vulnerability is not specific to the cloud.

Amazon and its AWS customers, including Capital One, employ a Shared Responsibility Model for security of data stored in AWS. Under this model, AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer, in this case Capital One, assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Configuration, testing and validation of the Capital One applications and data is performed by Capital One.

INTERROGATORY NO. 19:

Describe in detail Your relationship with Capital One, including any joint venture, dedicated resources with roles and responsibilities, scope of services, and exclusivity arrangements between You and Capital One and Capital One's participation in Your efforts to attract financial institutions and other large companies to host data on Your servers.

OBJECTIONS TO INTERROGATORY NO. 2:

Amazon Defendants object to this Interrogatory on the grounds that it seeks information that is irrelevant, immaterial or not proportional to the needs of the case. Amazon Defendants

object to this Interrogatory as compound and consisting of at least two distinct subparts. Amazon Defendants object to this Interrogatory on the grounds that it seeks documents from an overbroad and irrelevant time frame, including but not limited to January 1, 2015 to the present, and is thus unduly burdensome to the extent that it requests information outside of a time period relevant to the action. Amazon Defendants also object to the Interrogatory because the phrases "Your relationship with Capital One," "dedicated resources with roles and responsibilities," and "efforts to attract financial institutions and other large companies to host data on Your servers" are vague and ambiguous, and fail to sufficiently identify the specific information being sought. Additionally, Amazon Defendants object to the Interrogatory to the extent it broadly seeks information regarding Amazon Defendants' "relationship with Capital One" generally, without being tailored to any issues that might be relevant to the Breach or the claims and defenses at issue in this litigation.

RESPONSES TO INTERROGATORY NO. 19:

Subject to the foregoing objections, Amazon responds as follows:

Capital One has been an AWS customer since 2015. The history of Capital One's movement of its IT operations onto AWS is described at https://aws.amazon.com/solutions/case-studies/capital-one-enterprise/. The contract for Capital One's use of AWS is set forth in the Amended and Restated AWS Enterprise Customer Agreement effective February 1, 2015, as subsequently amended by the November 1, 2016 Amendment No. 1 and the Second Amended and Restated AWS Enterprise Customer Agreement, which became effective as of May 31, 2019 (collectively, the "Enterprise Agreement").

INTERROGATORY NO. 20:

Describe in detail Your development and marketing of Cloud Custodian, including listing the individuals responsible for its development and implementation, along with their titles, description of responsibilities, dates of employment, and, if no longer employed by You, their end date of employment and how they can be contacted.

OBJECTIONS TO INTERROGATORY NO. 2:

Amazon Defendants object that marketing of Cloud Custodian is not relevant to any claim or defense in the action. Amazon Defendants further object to this Interrogatory on the grounds that it seeks information that is not proportional to the needs of the case. Amazon Defendants object to this Interrogatory as compound and consisting of at least two distinct subparts. Amazon Defendants object to this Interrogatory as overbroad and unduly burdensome to the extent it seeks information regarding each and every individual involved in the development, implementation and marketing of Cloud Custodian. Amazon Defendants object to this Interrogatory to the extent that it seeks information that is more readily accessible to Capital One, which has control of its AWS environment.

RESPONSES TO INTERROGATORY NO. 20:

Subject to the foregoing objections, Amazon responds as follows:

Amazon did not develop Cloud Custodian.

March 2, 2020

/s/ *Robert R. Vieth*

Robert R. Vieth, Esq. (VSB No. 24304)
HIRSCHLER FLEISCHER, PC
8270 Greensboro Drive, Suite 700
Tysons Corner, Virginia 22102
T: (703) 584-8903
F: (703) 584-8901
Email: rvieth@hf-law.com

Local counsel for Defendants Amazon.com, Inc. and Amazon Web Services, Inc.

Laurence F. Pulgram (admitted *pro hac vice*)
Jedediah Wakefield (admitted *pro hac vice*)
Tyler G. Newby (admitted *pro hac vice*)
Vincent Barredo (admitted *pro hac vice*)
Armen N. Nercessian (admitted *pro hac vice*)
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone:415.875.2300
Facsimile:15. 281.1350
Email: lpulgram@fenwick.com
jwakefield@fenwick.com
tnewby@fenwick.com
vbarredo@fenwick.com
anercessian@fenwick.com

Counsel for Defendants Amazon.com, Inc. and Amazon Web Services, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on March 2, 2020, I caused the foregoing document to be served upon Plaintiffs' Lead Counsel and Local Counsel via electronic mail addressed as follows:

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel: (816) 714-7100
siegel@stuevesiegel.com

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUN, P.L.L.P.
100 Washington Avenue South, Suite 200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
210 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com

Steven T. Webster
WEBSTER BROOK LLP
300 N. Washington Street, Suite 404
Alexandria, Virginia 22314
Tel: (888) 987-9991
stwebster@websterbrook.com

And upon Defendants' Lead Counsel and Local Counsel via electronic mail addressed as follows:

David L. Balser
S. Stewart Haskins II
John C. Toro
Kevin J. O'Brien
Robert D. Griest
KING & SPALDING LLP
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140
dbalser@kslaw.com
shaskins@kslaw.com
jtoro@kslaw.com
kobrien@kslaw.com
rgriest@kslaw.com

Robert A. Angle
Tim St. George
Jon S. Hubbard
Harrison Scott Kelly
TROUTMAN SANDERS LLP
1001 Haxall Point
Richmond, VA 23219
Telephone: (804) 697-1200
Facsimile: (804) 697-1339
robert.angle@troutman.com
jon.hubbard@troutman.com
scott.kelly@troutman.com
timothy.st.george@troutman.com

Mary C. Zinsner (VSB No. 31397)
TROUTMAN SANDERS LLP
401 9th Street, NW, Suite 1000
Washington, DC 20004
Telephone: (703) 734-4334
Facsimile: (703) 734-4340
mary.zinsner@troutman.com

/s/ Margaret E. Vertin
Margaret E. Vertin